(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－161354

(43)公開日　平成６年(1994)６月７日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		8837－5L		
Ｇ０６Ｋ　17/00		Ｓ　7459－5L		

審査請求　未請求　請求項の数２(全 11 頁)

(21)出願番号　特願平4－317255

(22)出願日　平成４年(1992)11月26日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　石黒　銀矢
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　牟田　敏保
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　崎田　一貴
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

最終頁に続く

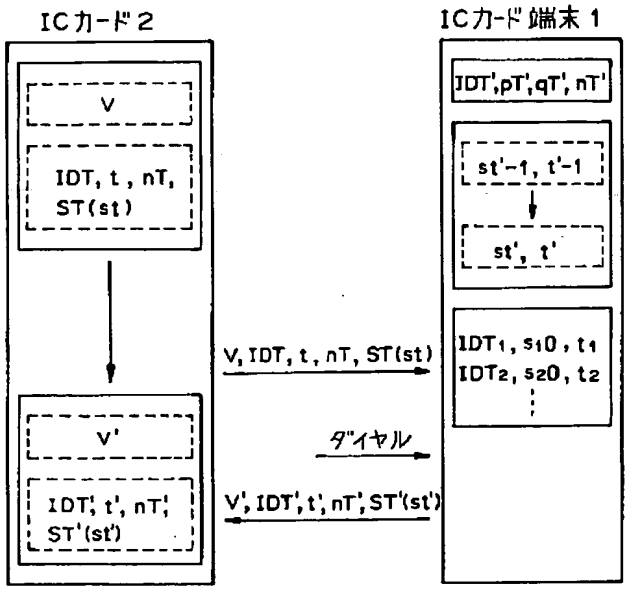
(54)【発明の名称】　ＩＣカード端末及びそれを用いたシステム

(57)【要約】　(修正有)

【目的】　ＩＣカード端末を用いた不正使用を防止する。

【構成】　ＩＣカード２をＩＣカード端末１に挿入すると、ＩＣカードから残金額Ｖと前回使用した端末の番号ＩＤＴ、タイムスタンプ情報ｓｔの更新回数を示す回数ｔ、公開鍵ｎＴ、タイムスタンプの署名ＳＴ（ｓｔ）とが端末へ送信される。盗難端末の番号と一致するものがなければＶが利用者により指定されたサービス料金より高ければサービスを提供。サービス終了後Ｖから使用料金を引いた残りＶ′と、その端末のＩＤＴ′、更新情報ｔ′、端末鍵ｐＴ′，ｑＴ′によるタイムスタンプ情報ｓｔ′に対するデジタル署名ＳＴ′（ｓｔ′）、公開鍵ｎＴ′とをＩＣカードへ送る。端末リストのＩＤＴ初期値を、受信したｔだけ繰り返し演算してタイムスタンプ情報を更新これと鍵ｎＴとにより署名ＳＴの正当性を検証、正当でなければ異常カードとし、正当であれば、ＩＣカードが端末で使用された時期を判定する。

図４



【特許請求の範囲】
【請求項１】　適当な間隔で所定のアルゴリズムによりタイムスタンプ情報を更新する手段と、
上記タイムスタンプ情報の更新ごとにその更新回数を表す更新情報を管理センタへ送信する手段と、
端末を特定するための端末番号、上記タイムスタンプ情報、上記更新情報、デジタル署名を作成するための端末鍵、上記デジタル署名を検証するための公開鍵とを記録したメモリと、
上記管理センタから受信した端末番号、タイムスタンプ情報の初期値、更新情報が端末リストとして記録されるメモリと、
ＩＣカードから受信した端末番号と上記端末リストの端末番号との比較を行い、一致しているとその端末リストのタイムスタンプ情報の初期値を、上記ＩＣカードから受信した更新情報に応じて上記所定のアルゴリズムにより更新し、その更新したタイムスタンプ情報と、受信した公開鍵とにより上記ＩＣカードから受信したデジタル署名の検証を行い、正当と判断したとき、上記受信した更新情報と上記一致した端末番号の端末リストの更新情報との比較を行い、上記ＩＣカードが上記受信した端末番号のＩＣカード端末で使用された時期を判断する手段と、
上記更新されたタイムスタンプ情報を上記端末鍵を用いてデジタル署名する手段と、
上記端末を特定するための端末番号、上記更新情報、上記公開鍵、上記デジタル署名を上記ＩＣカードへ送信する手段と、
を具備するＩＣカード端末。
【請求項２】　上記請求項１記載のＩＣカード端末と、
ＩＣカード端末から受信されたその端末番号、更新情報、公開鍵、タイムスタンプ情報に対するデジタル署名を記録するメモリと、
ＩＣカード端末へ挿入すると上記メモリ中の端末番号、更新情報、公開鍵、タイムスタンプ情報に対するデジタル署名をそのＩＣカード端末へ送信する手段とを具備するＩＣカードと、
各ＩＣカード端末の端末番号、タイムスタンプ情報の初期値及び更新情報を管理するデータベースと、
上記ＩＣカード端末より受信された更新情報に、上記データベース中の対応端末番号の更新情報を置き換える手段と、
上記データベース中の端末番号、タイムスタンプ情報の初期値及び更新情報の１組を選択してすべてのＩＣカード端末へ送信する手段と、を具備する管理センタと、
よりなるＩＣカードシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】この発明はＩＣカードをプリペイドカード、クレジットカード、スタンプカードなどとして使用するシステム、及びそのＩＣカード端末に関する。
【０００２】
【従来の技術】従来この種のシステムは、ＩＣカードとＩＣカード端末とが同じ暗号方式で、同じ秘密鍵を持ち、金額情報をこの秘密鍵で暗号化して通信し、各々の秘密鍵はＩＣカードやＩＣカード端末の内部を開けても、秘密鍵を見たり、改ざんしたりできないようにしていた。したがって、秘密鍵が漏洩しない限りＩＣカードの内容を改ざんすることはほとんど不可能であった。
【０００３】
【発明が解決しようとする課題】しかしながら、盗んだＩＣカード端末を用いてＩＣカードの内容を不正に書き換えることは不可能とは言えず、一旦可能となった場合にはシステムダウンといった重大な影響を及ぼす危険性がある。
【０００４】
【課題を解決するための手段】請求項１の発明は端末を特定するための端末番号、適当な間隔で所定のアルゴリズムにより更新されるタイムスタンプ情報、そのタイムスタンプ情報の更新回数を表す更新情報、デジタル署名を作成するための端末鍵、そのデジタル署名を検証するための公開鍵を記録したメモリ、管理センタから受信した端末番号、タイムスタンプ情報の初期値、更新情報を端末リストとして記録するためのメモリ、ＩＣカードから受信した端末番号と前記端末リストに記録している端末番号との比較を行い、一致したとき端末リストに記録しているその端末番号に対応するタイムスタンプ情報の初期値をＩＣカードから受信した更新情報にしたがい前記所定のアルゴリズムにより更新し、その更新したタイムスタンプ情報とＩＣカードから受信した公開鍵とにより受信したデジタル署名の検証を行い、正当と判断したとき、受信した更新情報と端末リストに記録しているその端末番号に対応する更新情報との比較を行い、そのＩＣカードが受信した端末番号のＩＣカード端末で使用された時期を判断する手段を持つＩＣカード端末である。
【０００５】請求項２の発明によれば請求項１の発明のＩＣカード端末と、ＩＣカード端末での使用後に、そのＩＣカード端末の前記端末番号、前記更新情報、前記タイムスタンプ情報を含む情報に対するデジタル署名、前記公開鍵を受信してメモリに記録する手段、次の使用時に、前記メモリに記録している端末番号、更新情報、デジタル署名、公開鍵をＩＣカード端末へ送信する手段を持つＩＣカードと、各ＩＣカード端末の端末番号、タイムスタンプ情報の初期値および更新情報を管理するデータベース、ＩＣカード端末がそのタイムスタンプ情報を更新するごとにそのＩＣカード端末から更新情報を受信し、その端末番号に対応して記録している更新情報を受信した更新情報に置き換える手段を持つ管理センタとによりＩＣカードシステムが構成されている。

【０００６】
【作用】このように構成しているから、ＩＣカードを使用したとき、ＩＣカード内の所定のメモリエリアに、使用したＩＣカード端末の端末番号、そのＩＣカード端末が作成したデジタル署名を検証するための公開鍵、使用時点のタイムスタンプ情報に対してそのＩＣカード端末が作成したデジタル署名、そのタイムスタンプ情報の更新情報とを記録する。次に別のＩＣカード端末で使用したとき、ＩＣカードは前記メモリに記録した情報をＩＣカード端末へ送信し、ＩＣカード端末は受信した端末番号から前回使用したＩＣカード端末を特定する。その端末番号とＩＣカード端末内の端末リストに登録されている端末番号との比較を行い、一致するものがあるとき、その端末リストに登録されているその端末番号に対応したタイムスタンプ情報の初期値と更新情報を読み出し、そのタイムスタンプ情報の初期値をＩＣカードから受信した更新情報にしたがって所定のアルゴリズムにより更新して前回使用した時点でのＩＣカード端末のタイムスタンプ情報を求める。その求めたタイムスタンプ情報とＩＣカードから受信した公開鍵とによりタイムスタンプ情報に対するデジタル署名の正当性を検証し、ＩＣカードから受信した更新情報が正しい値であることをチェックする。その更新情報が正当であるとき、その更新情報と前記端末リストに記録されている更新情報を比較し、ＩＣカードの前記端末リストに登録されているＩＣカード端末での使用時期が、前記端末リストに端末番号を登録した時点よりも以前か、以後かを判断する。デジタル署名の検証において正当性を検証できなかったときには、ＩＣカードから受信した更新情報あるいはデジタル署名が正規の情報ではないと判断し、異常カードとして処理する。さらに、管理センタでＩＣカード端末の端末番号を指定すれば、その端末番号のＩＣカード端末のタイムスタンプ情報の初期値、その時点での更新情報を知ることができ、それらの情報をＩＣカード端末の端末リストに登録することができる。
【０００７】
【実施例】次に図を参照してこの発明の一実施例をプリペイドカードシステムに適用した場合につき説明する。図１は請求項２の発明の一実施例のシステム構成の説明図であって、ＩＣカード端末１はＩＣカード２により料金処理を実施し、通話など各種サービスを提供する。管理センタ３はＩＣカード端末１の端末番号などを管理し、ＩＣカード端末１の電話番号へ発呼することによりＩＣカード端末１と管理センタ３とは通信網４を介して接続され、情報を送信することができる。
【０００８】図２は請求項１の発明のＩＣカード端末１の内部構成を示す図であり、制御部１１はＣＰＵからなり、処理手順、タイムスタンプ情報を更新するためのアルゴリズム、デジタル署名を作成するためのアルゴリズムなどのプログラムを内部のＲＯＭに記録しているとともに、端末番号、タイムスタンプ情報、タイムスタンプ情報の更新情報、デジタル署名を作成するための端末鍵、デジタル署名を検証するための公開鍵などを内部ＲＡＭに記録している。タイムスタンプ情報を更新するアルゴリズムとしては、例えば「電子情報通信学会論文誌Ｄ分冊，Ｊ７０－Ｄ，Ｎｏ．７，ｐ．１４１３～１４２３（１９８７）」に記載のＦＥＡＬを用いてもよく、デジタル署名のアルゴリズムとしては、例えば「ＮＴＴ Ｒ&Ｄ Ｖｏｌ．４０，Ｎｏ．５，ｐ．６８７～６９６（１９９１）」に記載のＥＳＩＧＮを用いることができる。端末番号、タイムスタンプ情報の初期値、端末鍵、公開鍵は、ＩＣカード端末設置時に、通信網を介して管理センタ３（図示せず）と接続し、管理センタ３から受信してメモリに記録してもよく、ＩＣカード端末製造時に予め設定してもよい。更新情報は例えば初期値として０を設定し、タイムスタンプ情報を更新するごとに１，２，…と増加していく。また、内部ＲＡＭには特定のＩＣカード端末の端末番号、タイムスタンプ情報の初期値、更新情報を登録するための端末リストエリアが設けられている。ＩＣカード２とデータのやりとりを行うＩＣカードリーダライタ部１２、操作ボタン、ダイヤルボタンなどからなる操作入力部１３、液晶ディスプレイからなる表示部１４、通話回路１５は制御部１１に接続され、通話回路１５に送受器１６が接続され、通信網との処理を行う通信処理部１７が制御部１１に接続されている。
【０００９】図３はＩＣカード２の内部構成を示す図であり、ＩＣカードの処理手順、デジタル署名の検証のためのアルゴリズム等のプログラムはＲＯＭ６１に記録され、ＣＰＵ６３はワークエリアとしてＲＡＭ６２を利用してすべての制御を行い、図２に示したＩＣカード端末１のＩＣカードリーダライタ部１２との通信は通信部６５により接点６６を介して行われる。金額情報はＩＣカード２の発行時にＩＣカード発行機（図示せず）によって書き込まれ、ＥＥＰＲＯＭ６４に記録されている。
【００１０】図１から図３の構成において、ＩＣカード端末１に設定した端末番号、タイムスタンプ情報の初期値、更新情報は管理センタ３に登録される。ＩＣカード端末１に設定したタイムスタンプ情報（初期値）は内部の時計機能により、例えば１日ごとに所定のアルゴリズムにより更新され、ｓ０→ｓ１→ｓ２→…ｓｔ…のごとく新しいタイムスタンプ情報に置き換えられ、前のタイムスタンプ情報は消滅する。このタイムスタンプ情報の更新は１定周期ごとでなくてもよく、つまり非周期的でもよい。タイムスタンプ情報を更新するごとに、更新した回数を更新情報として置き換える各タイムスタンプ情報と更新情報とが対応していればよく、つまりタイムスタンプ情報は単なる記号で、数量でなくても各更新回数とタイムスタンプ情報とが１対１で対応していればよい。更新情報を更新したとき、ＩＣカード端末１から管

理センタ３に自動発信し、端末番号と更新した更新情報を送信する。管理センタ３は登録されている対応端末番号の更新情報を、受信した更新情報に置き換える。なお、タイムスタンプ情報を更新する所定のアルゴリズムとしては、現在のタイムスタンプ情報から、前のタイムスタンプ情報を求めることができないようなアルゴリズムとすることが必要である。また、管理センタ３に登録されたタイムスタンプ情報の初期値は更新されない。このような状態において、ＩＣカード端末の盗難が発生した時、管理センタ３は盗まれたＩＣカード端末の端末番号から、そのＩＣカード端末のタイムスタンプ情報の初期値、盗まれた時点のタイムスタンプ情報の更新情報を知ることができ、それらの情報は管理センタ３からダウンロードにより全ＩＣカード端末１の端末リストに登録される。

【００１１】図４は利用者がＩＣカード２を使ってＩＣカード端末１からサービスを受けるときの処理を説明する図である。ＩＣカード２のＥＥＰＲＯＭ６４の所定のエリアに金額情報Ｖが記録され、他の所定のエリアには前回使用したＩＣカード端末の端末番号ＩＤＴ、公開鍵ｎＴ、更新情報ｔ、タイムスタンプ情報に対するデジタル署名ＳＴ（ｓｔ）が記録されている。また、ＩＣカード端末１の制御部１１内のＲＡＭの所定のエリアに端末番号ＩＤＴ′、デジタル署名用の端末鍵ｐＴ′，ｑＴ′、公開鍵ｎＴ′が記録され、他の所定のエリアにはタイムスタンプ情報ｓＴ′、更新情報ｔ′が記録されている。更に、ＩＣカード端末１の端末リストには、特定の端末の端末番号IDT_i（ｉ＝１，２，…）、タイムスタンプ情報の初期値s_i ０、更新情報t_iが記録されている。

【００１２】利用者がＩＣカード２をＩＣカード端末１のＩＣカードリーダライタ部１２に挿入するとＩＣカード２からＩＣカード端末１にＶ，ＩＤＴ，ｔ，ｎＴ，ＳＴ（ｓｔ）が送信される。ＩＣカード端末１は受信したＩＤＴと端末リスト内のデータIDT_iとの比較を行い、一致するものがない場合にはＶ及びガイダンスを表示部に表示する。利用者は表示部１４に表示されたガイダンスを参照して、操作入力部１３からダイヤルなどによりサービスを指定すると、ＩＣカード端末１は指定されたサービスの料金を制御部１１内のメモリに記憶されているリストの中から読み取るか、あるいは、通信網４を介して図示していないサービスセンタから受信し、この必要なサービス料金と残金額Ｖを比較して、Ｖが大きければサービスの提供を開始する。たとえば、電話サービスであれば残金額が１０円以上であればダイヤル指示を表示部１４に表示し、利用者のダイヤルに従って相手に発信する。利用者がサービスの提供を受け、例えば相手との通話が終ったサービス終了後は、ＩＣカード端末１は制御部１１内のメモリにあるサービス料金結果あるいはサービスセンタから送信されるサービス料金結果を前記残金額Ｖから減算して新しい残金額Ｖ′を求め、タイムスタンプ情報ｓｔ′に対してデジタル署名ＳＴ′（ｓｔ′）を端末鍵ｐＴ′，ｑＴ′で作成し、ＩＤＴ′，Ｖ′，ｔ′，ｎＴ′ＳＴ′（ｓｔ′）をＩＣカード２へ送信する。ＩＣカード２は残金額Ｖ′とともにＩＣカード端末１から受信した情報をＥＥＰＲＯＭ６４に記録する。

【００１３】上記の処理において、ＩＣカード端末１が受信したＩＤＴと一致するデータが端末リスト内のデータIDT_iにあった場合には、次の処理を行う。

①IDT_1が一致した端末番号とすると、端末リスト内の一致した端末番号に対応するタイムスタンプ情報の初期値s_1 ０を、ＩＣカード端末１のプログラムとして記録されている所定のアルゴリズムにより、ＩＣカード２から受信した更新情報ｔに従い、その更新回数だけ繰り返し演算を行い、このｔと対応したタイムスタンプ情報ｓ，ｔを求める。

【００１４】

s_1 ０→s_1 １→s_1 ２　　……→s_1 ｔ

②この演算により求めたタイムスタンプ情報st_1と、ＩＣカード２から受信した公開鍵ｎＴとによりデジタル署名ＳＴ（ｓｔ）の正当性の検証を行う。

③正当性が検証できなかった場合には、異常カードとして処理を中止し、ＩＣカード２を返却する。

④正当性が検証できた場合には、端末リスト内の一致した端末番号IDT_1に対応する更新情報t_1と、ＩＣカード２から受信した更新情報ｔとの比較を行う。

⑤ｔ≦t_1の場合には、そのｔはIDT_1，s_1 ０，t_1が端末リストに登録される前の更新情報であると、すなわちそのＩＣカードは、そのＩＤＴ$_1$のＩＣカード端末が盗難される前にそのＩＣカード端末でデータ（端末番号、更新情報、公開鍵、デジタル署名されたタイムスタンプ情報）が更新されたＩＣカードであると判断され、正当なものとして以降の処理を行う。

⑥ｔ＞t_1の場合には、そのt_1は、IDT_1，s_1 ０，t_1が端末リストに登録された後の更新情報であると、すなわちそのＩＣカードは、そのＩＤＴ$_1$のＩＣカード端末が盗難された後にそのＩＣカード端末でデータが更新されたＩＣカードであると判断され、不正カードとして処理を中止し、返却あるいはＩＣカード端末内への留置処理を行う。

【００１５】図５はこの発明の他の実施例を説明する図であって、ＩＣカード２のＲＯＭ６１にはデジタル署名を作成するためのアルゴリズム、乱数を生成するためのアルゴリズムが記録されている。また、ＩＣカード２のＥＥＰＲＯＭ６４にはカード番号ＩＤＵ、デジタル署名を作成するためのカード鍵ｐＵ，ｑＵ，デジタル署名を検証するための公開鍵ｎＵが記録されている。ＥＥＰＲＯＭ６４の所定のエリアには前回使用したＩＣカード端末の端末番号ＩＤＴ、公開鍵ｎＴ、更新情報ｔ、前回の

使用時に生成された乱数ＲおよびＸ、とともにこれら乱数Ｒ，Ｘ、金額情報Ｖ、カード番号ＩＤＵに対して前回使用したＩＣカード端末が作成した第１のデジタル署名ＳＴ（Ｒ＊Ｘ＊Ｖ＊ＩＤＵ）、そのデジタル署名およびタイムスタンプ情報ｓｔに対して前回使用したＩＣカード端末が作成した第２のデジタル署名ＳＴ（ｓｔ＊ＳＴ（Ｒ＊Ｘ＊Ｖ＊ＩＤＵ））が記録されている。また、ＩＣカード端末１の制御部１１内のＲＯＭには乱数を生成するためのアルゴリズムが記録されている。

【００１６】利用者がＩＣカード２をＩＣカード端末１のＩＣカードリーダライタ部１２に挿入すると、ＩＣカード２からＩＣカード端末１に前回使用情報であるＲ，Ｘ，Ｖ，ＩＤＵ、第１のデジタル署名、ＩＤＴ，ｔ，ｎＴ、第２のデジタル署名が送信される。ＩＣカード端末１は受信したｎＴにより第１のデジタル署名の正当性を検証する。正当であれば、受信した端末番号ＩＤＴと端末リスト内のデータとの比較を行い、一致するものがない場合には乱数Ｒ′を生成しＩＣカードへ送信する。ＩＣカードでは乱数Ｘ′を生成するとともにＲ′，Ｘ′，Ｖに対して鍵ｐＵ，ｑＵによりデジタル署名ＳＵ（Ｒ′＊Ｘ′＊Ｖ）を作成し、Ｘ′，ＳＵ（Ｒ′＊Ｘ′＊Ｖ）、ｎＵをＩＣカード端末１へ送信する。ＩＣカード端末１では受信した公開鍵ｎＵによりデジタル署名ＳＵ（Ｒ′＊Ｘ′＊Ｖ）の正当性を検証する。正当であればＶを表示部に表示し所定のサービスを提供する。そのサービス終了後、新しい残金額Ｖ′を求め、Ｒ′，Ｘ′，Ｖ′，ＩＤＵに対して鍵ｐＴ′，ｑＴ′により第１のデジタル署名ＳＴ′（Ｒ′＊Ｘ′＊Ｖ′＊ＩＤＵ）を作成するとともに、タイムスタンプ情報ｓｔ′と第１のデジタル署名に対して第２のデジタル署名ＳＴ′（ｓｔ′＊ＳＴ（Ｒ′＊Ｘ′＊Ｖ′＊ＩＤＵ））を作成し、Ｖ′，ＩＤＴ′，ｎＴ，ｔ′、第１のデジタル署名、第２のデジタル署名をＩＣカード２へ送信する。ＩＣカード２は受信したｎＴ′により受信した第１のデジタル署名の検証を行い、正当であれば受信した情報を所定のエリアに記録する。以上の手順でデジタル署名の正当性が検証できなかった場合にはその時点で処理を中止し、ＩＣカード２を返却する。

【００１７】上記の処理において、ＩＣカード端末１が受信したＩＤＴと一致するデータが端末リスト内のデータ$ＩＤＴ_i$にあった場合には、前述した処理と同様の処理を行う。この実施例では情報の送受に相互に生成した乱数を使用しているため信号の内容は同一となることはなく、傍受した信号を利用した不正を防止することができる。また、相互にデジタル署名を作成して相互認証を行っているためセキュリティをより高めることができる。なお情報の数が多い程、セキュリティが高くなるが、カード番号ＩＤＵを省略しても図４の場合より可成りよくなる。

【００１８】以上の説明において、ＩＣカード端末１およびＩＣカード２はそれぞれ端末番号およびカード番号のみメモリに記録しているように説明してきたが、特定の鍵情報によって端末番号およびカード場合のデジタル署名を作成し、そのデジタル署名を検証鍵とともに各々のメモリに記録しておき、端末番号あるいはカード番号とともにそのデジタル署名、検証鍵も一緒に送信し、検証鍵によりデジタル署名を検証することにより端末番号あるいはカード番号の正当性を検証するように構成すればセキュリティをより高めることができる。

【００１９】また、ＩＣカード２およびＩＣカード端末１に送信情報の暗号化・復号化のためのアルゴリズムと暗号化および復号化のための共通の鍵をメモリに記憶しておくことにより、相互の通信を暗号通信により行うことができ、よりセキュリティを高めることができる。

【００２０】

【発明の効果】この発明によれば、ＩＣカード端末が設置されてからの経過時間を表す更新情報と、更新情報の正当性を検証するためのタイムスタンプ情報をＩＣカード端末に記録し、ＩＣカードを使用すると、更新情報とともにタイムスタンプ情報の正当性を検証するためのそのＩＣカード端末のデジタル署名をＩＣカードに記録するため、ＩＣカードの内容を解析して更新情報をもどすように改ざんしたとしても、その改ざんした更新情報と対応するタイムスタンプ情報に対するＩＣカード端末のデジタル署名を作成することができないために不正はできない。また、ＩＣカード端末の内容を解析して更新情報をもどすように改ざんしたとしても、もどした更新情報に対応するタイムスタンプ情報を得ることはできず、不正を行うことはできない。ＩＣカード端末の解析によりできることは、その時点以降のタイムスタンプ情報、更新情報の付いた内容の改ざんとなり、他のＩＣカード端末で使用した場合には、端末リストチェックにより不正を防ぐことができる。

【図面の簡単な説明】

【図１】請求項２の発明の一実施例のシステム構成を示すブロック図。

【図２】請求項１の発明のＩＣカード端末の構成例を示すブロック図。

【図３】ＩＣカードの構成例を示すブロック図。

【図４】この発明の情報処理手順の例を示す図。

【図５】この発明の他の情報処理手順を示す図。

【図１】

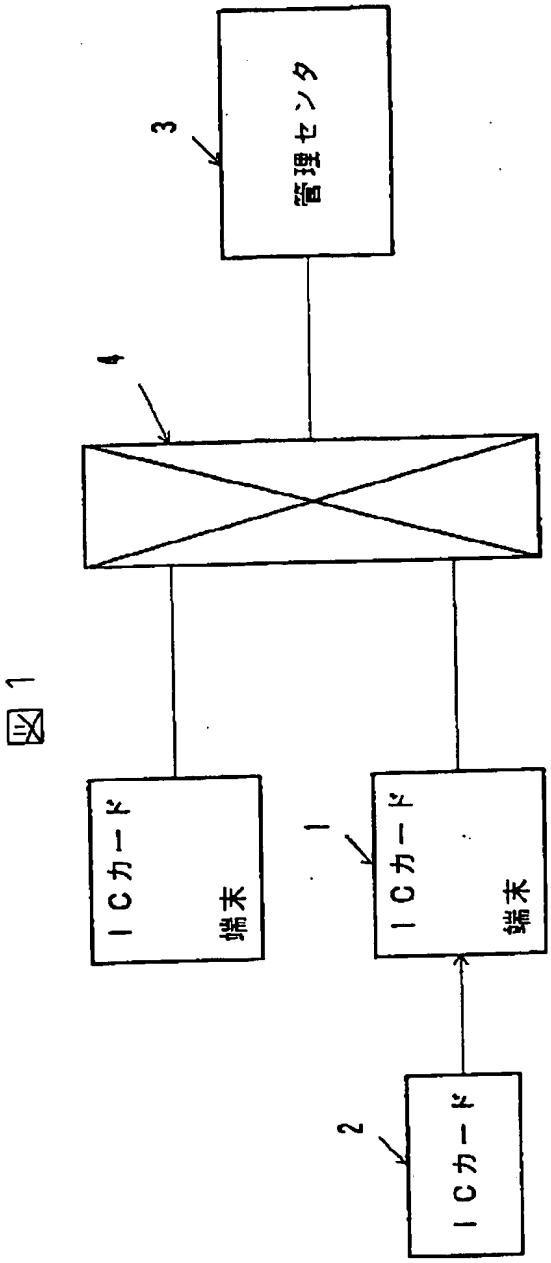
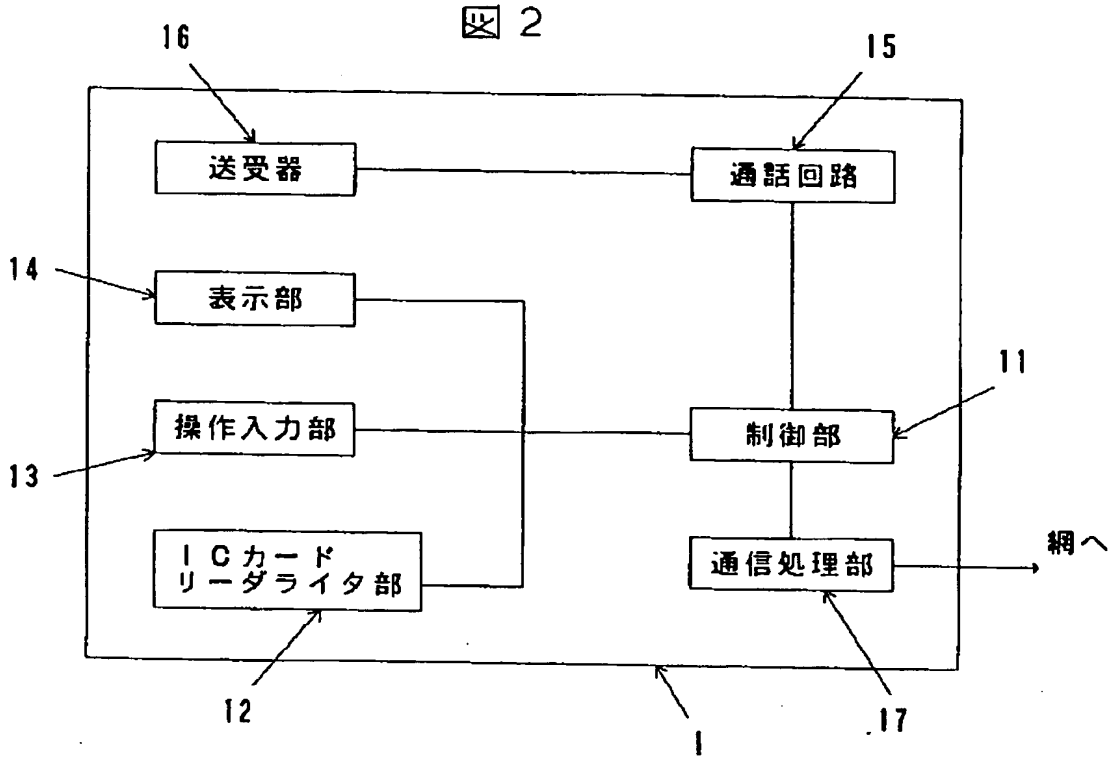


図１

【図2】

図 2


16
15
送受器
通話回路
14
表示部
11
操作入力部
制御部
13
ＩＣカード
リーダライタ部
通信処理部
網へ
12
1
17

【図3】

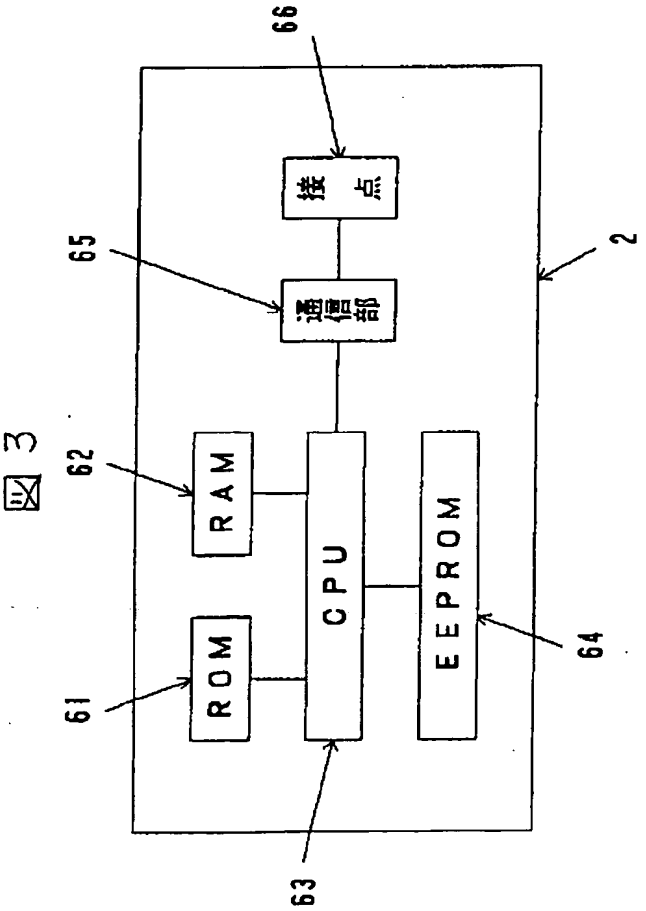
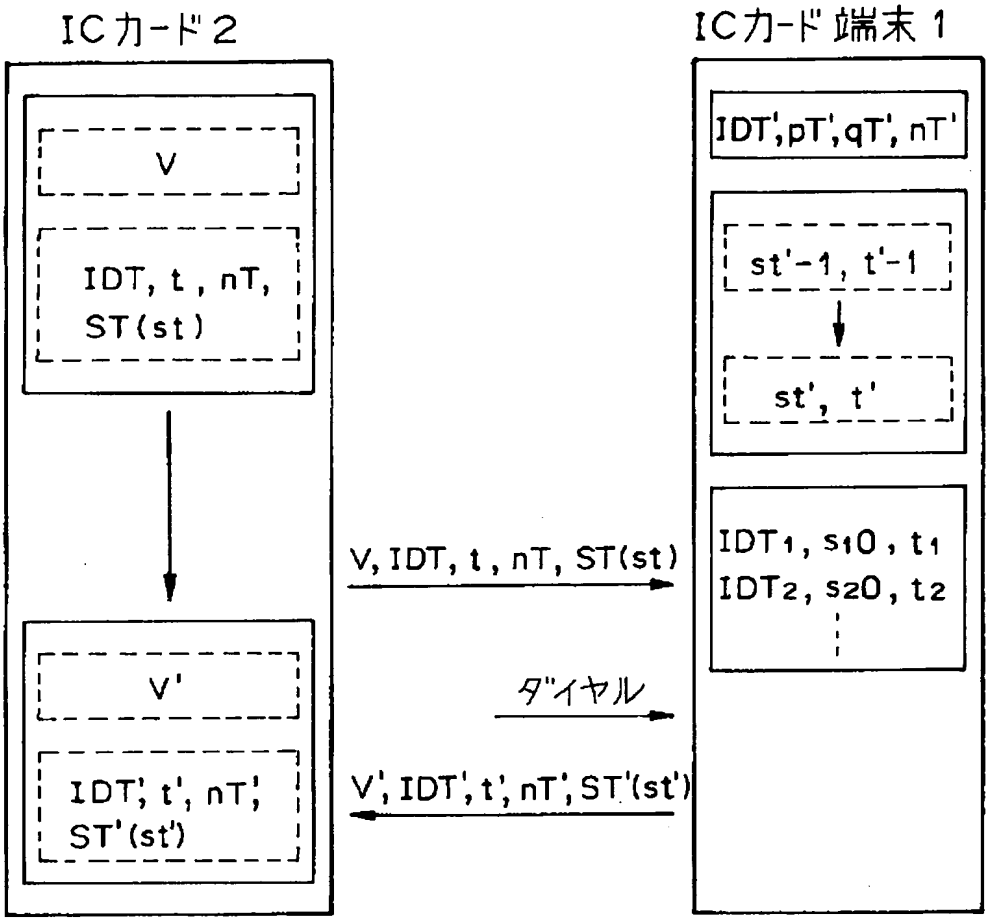


図3

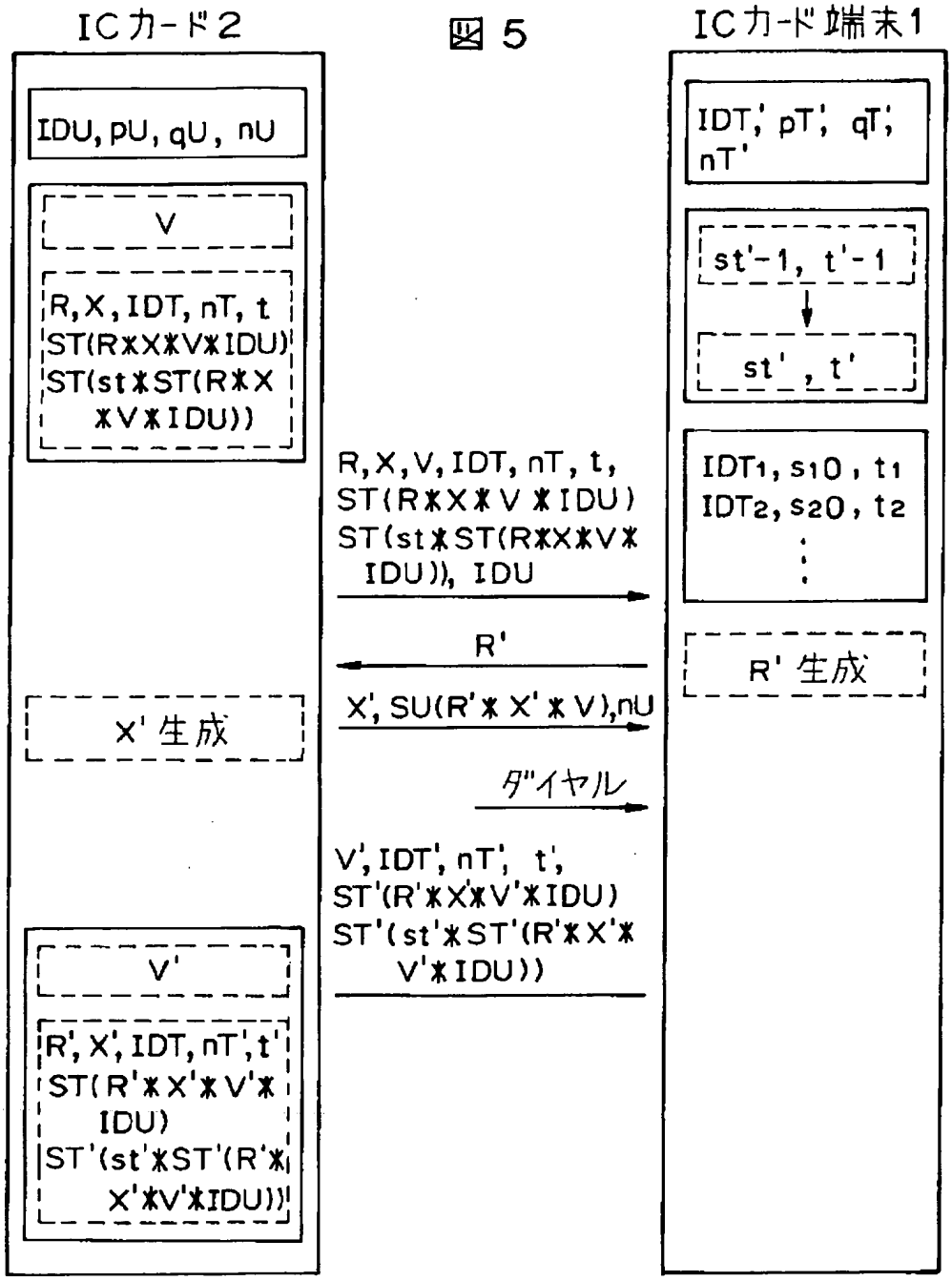
【図4】

図 4


ICカード2
V
IDT, t , nT,
ST(st)
V'
IDT', t', nT',
ST'(st')
ICカード端末 1
IDT',pT',qT', nT'
st'-1, t'-1
st', t'
IDT1, s10 , t1
IDT2, s20, t2
V, IDT, t , nT, ST(st)
ダイヤル
V', IDT', t', nT', ST'(st')

【図5】

図5



フロントページの続き

(72)発明者　宮口　庄司
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　岡本　龍明
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　藤岡　淳
東京都千代田区内幸町１丁目１番６号　日
本電信電話株式会社内